Order Code RL30153

CRS Report for Congress

Critical Infrastructures: Background and Early Implementation of PDD-63

Updated June 19, 2001

John D. Moteff
Specialist in Science and Technology Policy
Resources, Science, and Industry Division

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
19 JUN 2001		**00-00-2001 to 00-00-2001**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Critical Infrastructures: Background and Early Implementation of PDD-63	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service,The Library of Congress,101 Independence Ave, SE,Washington,DC,20540-7500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**27**	

Critical Infrastructures: Background and Early Implementation of PDD-63

Summary

The nation's health, wealth, and security rely on the supply and distribution of certain goods and services. The array of physical assets, processes and organizations across which these goods and services move are called critical infrastructures (e.g. electricity, the power plants that generate it, and the electric grid upon which it is distributed or financial capital, the institutions that manage it, and the record- keeping and communications that move it from one institution to another). Computers and communications, themselves critical infrastructures, are increasingly tying these infrastructures together. There is concern that this reliance on computers and computer networks makes the nation's critical infrastructures vulnerable to "cyber" attacks. In May 1998, President Clinton released Presidential Decision Directive No. 63. The Directive sets up groups within the federal government to develop and implement plans that would protect government-operated infrastructures and calls for a dialogue between government and the private sector to develop a National Infrastructure Assurance Plan that would protect the nation's critical infrastructures by the year 2003.

PDD-63 identified 12 areas critical to the functioning of the country: information and communications; banking and finance; water supply; transportation; emergency law enforcement; emergency fire service; emergency medicine; electric power, oil, and gas supply and distribution; law enforcement and internal security; intelligence; foreign affairs; and national defense. The Directive assigned a lead agency to each sector to coordinate efforts at protecting the infrastructure upon which each of these areas depend. Where private operators are involved, the lead agency is responsible for identifying private sector coordinators with whom to work to develop a National Plan (on January 7, 2000 the Clinton Administration released Version 1.0 of this National Plan which pertains primarily to the government sector). The Directive ultimately envisions a national early warning and response capability, where cyber attacks can be detected, warnings issued, and responses coordinated. It calls for the private sector to set up Information Sharing and Analysis Centers that would allow them to participate in this national effort.

In its FY2001 budget, the Clinton Administration estimated that they requested $2.03 billion for activities related to critical infrastructure protection. While much of this funding is buried within ongoing operating and equipment accounts, making it difficult to track during the appropriations process, there were a few high visibility initiatives. These included $25 million to set up a Federal Cyber Services Training and Education program, $10 million to begin a pilot Federal Intrusion Detection Network, and $50 million to establish an Institute for Information Infrastructure Protection. Congress provided mixed support for these initiatives. PDD-63 and its implementation raise a number of issues. Among them is the ability and willingness of the private sector to cooperate with the federal government in sharing information. To what extent will the federal government get involved in the monitoring of privately operated infrastructures and what are the privacy implications? Costs are also unknown. And, it is unclear at this time whether the Bush Administration will reaffirm PDD-63 or pursue a different strategy.

Contents

List of Tables

Critical Infrastructures: Background and Early Implementation of PDD-63

Latest Developments

The Bush Administration is still reviewing its options for overseeing and coordinating protection of the nation's critical infrastructures. To date, the Administration has ruled out creating a singular federal Chief Information Officer or creating a new office or agency dedicated to homeland defense, both of which had been mentioned as possible places to put critical infrastructure protection responsibilities (see **Restructuring by the Bush Administration** on page 15).

The General Accounting Office recently released a report (May 22) evaluating the progress made by the National Infrastructure Protection Center in meeting the mission assigned it in PDD-63.

Introduction

Certain socio-economic activities are vital to the day-to-day functioning and security of the country; for example, transportation of goods and people, communications, banking and finance, and the supply and distribution of electricity and water. These activities and services have been referred to as components of the nation's critical infrastructure. Domestic security and our ability to monitor, deter, and respond to outside hostile acts also depend on some of these activities as well as other more specialized activities like intelligence gathering and command and control of police and military forces. A serious disruption in these activities and capabilities could have a major impact on the country's well-being.[1]

These activities and capabilities are supported by an array of physical assets, processes, information, and organizations forming what is being called the nation's critical infrastructures. The country's critical infrastructures are growing increasingly complex, relying on computers and, now, computer networks to operate efficiently and reliably. The growing complexity and the interconnectedness resulting from networking means that a disruption in one may lead to disruptions in others.

Disruptions can be caused by any number of factors: poor design, operator error, physical destruction due to natural causes, (earthquakes, lightening strikes, etc.) or

---

[1]As a reminder of how dependent society is on its infrastructure, in May 1998, PanAmSat's Galaxy IV satellite's on-board controller malfunctioned, disrupting service to an estimated 80-90% of the nation's pagers, causing problems for hospitals trying to reach doctors on call, emergency workers, and people trying to use their credit cards at gas pumps, to name but a few.

physical destruction due to intentional human actions (theft, arson, sabotage, etc.). Over the years, operators of these infrastructures have taken measures to guard against and to quickly respond to many of these risks. However, the growing dependency of these systems on information technologies and computer networks introduces a new vector by which problems can be introduced.[2]

Of particular concern is the threat posed by "hackers" who can gain unauthorized access to a system and who could destroy, corrupt, steal, or monitor information vital to the operation of the system. Unlike arsonists or saboteurs, hackers can gain access from remote locations. The ability to detect and deter their actions is still being developed. While infrastructure operators are also taking measures to guard against and respond to cyber attacks, there is concern that the number of "on-line" operations is growing faster than security awareness and the use of sound security measures.

Hackers range from mischievous teenagers, to criminals, to spies, to foreign military organizations. While the more commonly reported incidents involve mischievous teenagers (or adults) or self-proclaimed "electronic anarchists", the primary concern is that criminals, spies, and military personnel from around the world who appear to be perfecting their hacking skills and who may pose a potential strategic threat to the reliable operations of our critical infrastructures.[3]

The President's Commission on Critical Infrastructure Protection

In the FY1996 Department of Defense Authorization bill (P.L. 104-106) Congress required the President to report to Congress a national policy on protecting the nation's information infrastructure from strategic attack. Partially in response to that legislation and also to internal discussions on national security, President Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1996. Its tasks were to: report to the President the scope and nature of the vulnerabilities and threats to the nation's critical infrastructures (focusing primarily on cyber threats); recommend a comprehensive national policy and implementation plan for protecting critical infrastructures; determine legal and policy issues raised by proposals to increase protections; and propose statutory and regulatory changes necessary to effect recommendations.

---

[2]Efforts to merge the computer systems of Norfolk Southern and Conrail after their merger in June, 1999 caused a series of mishaps leaving trains misrouted, crews misscheduled, and products lost. As of January 2000, problems still persisted. See, "Merged Railroads Still Plagued by IT Snafus," Computerworld, January 17, 2000, pp 20-21.

[3]The Director of the Central Intelligence Agency testified before the Senate Committee on Governmental Affairs (June 24, 1998) that a number of countries are incorporating information warfare into their military doctrine and training and developing operational capability. It should be noted that the U.S. military is probably the leader in developing both offensive and defensive computer warfare techniques and doctrine.

The PCCIP released its report to President Clinton in October 1997.[4] While the Commission found no immediate crisis threatening the nation's infrastructures, it did find reason to take action. The rapid growth of a computer-literate population (implying a greater pool of potential hackers), the inherent vulnerabilities of common protocols in computer networks, the easy availability of hacker "tools" (available on many websites), and the fact that the basic tools of the hacker (computer, modem, telephone line) are the same essential technologies used by the general population indicated to the Commission that the threat and vulnerability exist.

The Commission's general recommendation was that greater cooperation and communication between the private sector and government was needed. Much of the nation's critical infrastructure is owned and operated by the private sector. As seen by the Commission, the government's primary role (aside from protecting its own infrastructures) is to collect and disseminate the latest information on intrusion techniques, threat analysis, and ways to defend against hackers.

The Commission also proposed a strategy for action:

- facilitate greater cooperation and communication between the private sector and appropriate government agencies by: setting a top level policy-making office in the White House; establishing a council that includes corporate executives, state and local government officials, and cabinet secretaries; and setting up information clearinghouses;
- develop a real-time capability of attack warning;
- establish and promote a comprehensive awareness and education program;
- streamline and clarify elements of the legal structure to support assurance measures (including clearing jurisdictional barriers to pursuing hackers electronically); and,
- expand research and development in technologies and techniques, especially technologies that allow for greater detection of intrusions.

The Commission's report underwent interagency review to determine how to respond. That review led to a Presidential Decision Directive released in May 1998.

Presidential Decision Directive No. 63

Presidential Decision Directive No. 63 (PDD-63)[5] set as a national goal the ability to protect the nation's critical infrastructure from intentional attacks (both physical and cyber) by the year 2003. According to the PDD, any interruptions in the ability of these infrastructures to provide their goods and services must be "brief,

---

[4]President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October 1997.

[5]See, *The Clinton's Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, White Paper, May 22, 1998, which can be found on [http://www.ciao.gov/ciao_document_library/paper598.html].

infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."[6]

PDD-63 identified the following activities whose critical infrastructures should be protected: information and communications; banking and finance; water supply; aviation, highways, mass transit, pipelines, rail, and waterborne commerce; emergency and law enforcement services; emergency, fire, and continuity of government services; public health services; electric power, oil and gas production, and storage. In addition, the PDD identified four activities where the federal government controls the critical infrastructure: internal security and federal law enforcement; foreign intelligence; foreign affairs; and national defense.

A lead agency was assigned to each of these "sectors" (see **Table 1**). Each lead agency was to appoint a **Sector Liaison Official** to interact with appropriate private sector organizations. The private sector was encouraged to select a **Sector Coordinator** to work with the agency's sector liaison official. Together, the liaison official, sector coordinator, and all affected parties will contribute to a sectoral security plan which will be integrated into a **National Infrastructure Assurance Plan** (see below). Each of the activities performed primarily by the federal government also are assigned a lead agency who will appoint a **Functional Coordinator** to coordinate efforts similar to those made by the Sector Liaisons.

Table 1. Lead Agencies

Department/Agency	Sector/Function
Commerce	Information and Communications
Treasury	Banking and Finance
EPA	Water
Transportation	Transportation
Justice	Emergency Law Enforcement
Federal Emergency Management Agency	Emergency Fire Service
Health and Human Services	Emergency Medicine
Energy	Electric Power, Gas, and Oil
Justice	Law Enforcement and International Security
Director of Central Intelligence	Intelligence
State	Foreign Affairs
Defense	National Defense

[6]Ibid.

The PDD created the position of **National Coordinator** for Security, Infrastructure Protection, and Counter-terrorism, who reports to the President through the Assistant to the President for National Security Affairs.[7] Among his many duties the National Coordinator chairs the **Critical Infrastructure Coordination Group**. This Group is the primary interagency working group for developing and implementing policy and for coordinating the federal government's own internal security measures. The Group includes high level representatives from the lead agencies (including the Sector Liaisons), the National Economic Council, and all other relevant agencies.

Each federal agency is responsible for securing its own critical infrastructure and shall designate a Critical Infrastructure Assurance Officer (CIAO) to assume that responsibility. The agency's current Chief Information Officer (CIO) may double in that capacity. In those cases where the CIO and the CIAO are different, the CIO is responsible for assuring the agency's information assets (databases, software, computers), while the CIAO is responsible for any other assets that make up that agency's critical infrastructure. The lead agencies listed in the Directive and others listed as primary agencies (Federal Bureau of Investigations, Central Intelligence Agency, Veterans Affairs, and the National Security Agency) were given 180 days from the signing of the Directive to develop their plans. Those plans are to be fully implemented within 2 years and updated every 2 years.

The PDD set up a **National Infrastructure Assurance Council**. The Council will be a panel that includes private operators of infrastructure assets and officials from state and local government officials and relevant federal agencies. The Council will meet periodically and provide reports to the President as appropriate. The National Coordinator will act as the Executive Director of the Council.

The PDD also called for a **National Infrastructure Assurance Plan**. The Plan is to integrate the plans from each of the sectors mentioned above and should consider the following: a vulnerability assessment, including the minimum essential capability required of the sector's infrastructure to meet its purpose; remedial plans to reduce the sector's vulnerability; warning requirements and procedures; response strategies; reconstitution of services; education and awareness programs; research and development needs; intelligence strategies; needs and opportunities for international cooperation; and legislative and budgetary requirements.

The PDD also set up a National Plan Coordination Staff to support the plan's development. This function is performed by the **Critical Infrastructure Assurance Office** (CIAO, not to be confused with the agencies' Critical Infrastructure Assurance Officers) and was placed in the Department of Commerce. CIAO supports the National Coordinator's efforts to integrate the sectoral plans into a National Plan, supports individual agencies in developing their internal plans, helps coordinate a national education and awareness programs, and provides legislative and public affairs support.

---

[7]President Clinton designated Richard Clarke, Special Assistant to the President for Global Affairs, National Security Council, as National Coordinator.

In addition to the above activities, the PDD called for studies on specific topics. These include issues of: liability that might arise from private firms participating in an information sharing process; legal impediments to information sharing; classification of information and granting of clearances (efforts to share threat and vulnerability information with private sector CEOs has been hampered by the need to convey that information in a classified manner); information sharing with foreign entities; and the merits of mandating, subsidizing or otherwise assisting in the provision of insurance for selected infrastructure providers.

Most of the Directive established policy-making and oversight bodies making use of existing agency authorities and expertise. However, the PDD also addressed operational concerns. The Directive called for a national capability to detect and respond to attacks while they are in progress. Although not specifically identified in the Directive, the Clinton Administration proposed establishing a **Federal Instruction Detection Network (FIDNET)**, that would, together with the **Federal Computer Intrusion Response Capability (FedCIRC)** effort begun just prior to PDD-63, meet this goal. The Directive did explicitly give the Federal Bureau of Investigation the authority to expand its existing computer crime capabilities into a **National Infrastructure Protection Center (NIPC)**. According to the Directive, the NIPC is to be the focal point for federal threat assessment, vulnerability analysis, early warning capability, law enforcement investigations, and response coordination. All agencies are required to forward to the NIPC information about threats and actual attacks on their infrastructure as well as attacks made on private sector infrastructures of which they become aware. Presumably, FIDNET[8] and FedCIRC would feed into the NIPC. According to the Directive, the NIPC would be linked electronically to the rest of the federal government and use warning and response expertise located throughout the federal government.. According to the Directive, the NIPC will also be the conduit for information sharing with the private sector through equivalent **Information Sharing and Analysis Center(s)** operated by the private sector.

While the FBI was given the lead, the NIPC also includes the Department of Defense, the Intelligence Community, and a representative from all lead agencies. Depending on the level of threat or the character of the intrusion, the NIPC may be placed in direct support of either the Department of Defense or the Intelligence Community.

Implementing PDD-63: Status As February, 2001

Selection of Sector Liaison Officials and Functional Coordinators. All lead agencies and lead functional agencies have appointed their Sector Liaison Officials and Functional Coordinators.

---

[8]From the beginning FIDNET generated controversy both inside and outside the government. Besides privacy concerns, cost, and technical feasibility were at issue. By the end of the Clinton Administration, FIDNET as a centralized intrusion detection system feeding into an analysis and warning capability was abandoned. Each agency, however, is allowed and encouraged to use intrusion detection technology to monitor and secure their own systems.

Identifying and Selecting Sector Coordinators. The identification of sector coordinators is proceeding with mixed results. The table below shows those individuals or groups that have agreed to act as Coordinators or have been approached by the lead agency.

Different sectors present different challenges to identifying a coordinator. Some sectors are more diverse than others (e.g. transportation includes rail, air, waterways, and highways; information and communications include computers, software, wire and wireless communications) and raises the issue of how to have all the relevant players represented. Other sectors are fragmented consisting of small or local entities. Some sectors, such as banking, telecommunications, and energy have more experience than others in working with the federal government and/or working collectively to assure the performance of their systems.

Besides such structural issues are ones related to competition. Inherent in the exercise is asking competitors to cooperate. In some cases it is asking competing industries to cooperate. This cooperation not only raises issues of trust among firms, but also concerns regarding anti-trust rules. Also, having these groups in direct communications with the federal government raises questions about their relationship to the federal government as governed by the Federal Advisory Committee Act (5 USC Appendix) and how the Freedom of Information Act (5 USC 552) applies to them and the information that may be exchanged.

For the most part, the sector coordinators selected to date have undertaken awareness and education activities not only to acquaint their constituents with the threats and risks of cyber attack on their systems (which in many cases is already known) but also about the efforts and goals of PDD-63. Typically these activities have been carried out through regular trade/professional association committee meetings, conferences, etc.

Sector coordinators have been identified for most of the major privately operated sectors. The Association of American Railroads is the most recent to accept the duties of coordinator for the rail sector. The Department of Transportation would like to also find coordinators for air and water transportation. FEMA has not identified a single coordinator to represent the country's emergency/fire service providers. FEMA is also responsible for the area of continuity of government. Again, no single coordinator has been identified, but FEMA had discussed continuity of government issues with state and local governments in the context of the Y2K.[9] Nor has the Department of Health and Human Services identified a central coordinator for the emergency medical community. The Department of Justice also has not identified a single coordinator for emergency law enforcement but is using existing outreach programs at the FBI and the NIPC to promote awareness and education activities.

---

[9]The New Mexico Critical Infrastructure Assurance Council, an offshoot of the FBI's InfraGard efforts in the state, include the state government and other state and local agencies. The Council is referenced in the *National Plan for Information Systems Protection*. See, **National Critical Infrastructure Plan**, below.

Table 2. Sector Coordinators

Lead Agency	Identified Sector Coordinators
Commerce	A consortium of 3 associations: Information Technology Assn. of America; Telecommunications Industry Assn.; U.S. Telephone Assn.
Treasury	Steven Katz - Citigroup
EPA	Assn. of Metropolitan Water Agencies
Energy	North American Electric Reliability Council and National Petroleum Council
Transportation	Association of American Railroads
Health and Human Services	
FEMA	
Justice	

Appointment of the National Infrastructure Assurance Council. The Administration released an Executive Order (13130) in July, 1999, formally establishing the council. Just prior to leaving office, President Clinton put forward the names of 18 people for nomination.[10]

Selection of Agency CIAOs. All agencies have made permanent or acting CIAO appointments.

Internal Agency Plans. All of the lead and primary agencies designated in PDD-63 met the initial deadline for submitting their internal plans for protecting their own critical infrastructures from attacks and for responding to intrusions. The Critical Infrastructure Assurance Office assembled an expert team to review the plans. The plans were assessed in 12 areas including schedule/milestone planning, resource requirements, and knowledge of existing authorities and guidance. The assessment team handed back the initial plans with comments. Agencies were given 90 days to respond to these comments.

A second tier of agencies identified by the National Coordinator were also required to submit plans. These were Agriculture, Education, Housing and Urban Development, Labor, Interior, General Services Administration, National Aeronautics and Space Administration and the Nuclear Regulatory Commission. Their plans were turned in by the end of February, 1999. These, too, were reviewed by the team and sent back with comments. Of the 22 agencies required to submit plans, 16 resubmitted plans in response to first round comments.

---

[10]White House Press Release, dated January 18, 2000.

Initially the process of reviewing these agency plans was to continue until all concerns were addressed. Over the summer of 1999, however, review efforts slowed and subsequent reviews were put on hold as the efficacy of the reviews was debated. Some within the CIAO felt that the plans were too general and lacked a clear understanding of what constituted a "critical asset" and the interdependencies of those assets. As a result of that internal debate, the CIAO has redirected its resources to institute a new program called Project Matrix. Project Matrix is a three step process by which an agency can identify and assess its most critical assets, identify the dependencies of those assets on other systems, including those beyond the direct control of the agency, and prioritize. CIAO has offered this analysis to 14 agencies, some not bound to PDD-63 (e.g. Social Security Administration and the Securities and Exchange Commission). Participation by the agencies are voluntary. Responsibility for review of agency critical infrastructure plans has been given to the National Institute of Standards and Technology, the support for which appeared in the Clinton Administration's FY2001 budget request (see Appendix).

According to the National Plan released in January 2000 (see below), all primary and secondary agencies are to have completed preliminary vulnerability analyses and to have outlined proposed remedial actions. Again, according to the National Plan, those remedial actions were to be budgeted for and submitted as part of the agencies' FY2001 budgets submissions to the Office of Management and Budget and every year thereafter. However, given the discussion above, the comprehensiveness of these plans at this time may be in question.

National Critical Infrastructure Plan. The Clinton Administration, after some delay, released Version 1.0 of its National Plan for Information Systems Protection in January 2000. The Plan focuses primarily on efforts within the federal government, and dividing those between government-wide efforts and those unique to the national security community. The Plan (159 pages) will not be summarized here in any detail. The reader is referred to the CIAO website ([http://www.ciao.gov]) for either the executive summary or the full text of the Plan. Essentially, the Plan identifies 10 "programs" under three broad objectives (see Table 3, below).

Each program contains some specific actions to be taken, capabilities to be established, and dates by which these shall be accomplished. Other activities, capabilities, and dates are more general (e.g. during FY2001).

The Plan includes a number of new initiatives identified by the Clinton Administration. These are identified in the appendix of this report. Of course, the ability to meet some of these milestones will depend on the willingness of Congress to appropriate funds to carry them out.

Table 3. National Plan for Information Systems Protection Version 1.0

Goal: Achieve a critical information systems defense with an initial operating capability by December 2000, and a full operating capability by May 2003...that ensures any interruption or manipulation of these critical functions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.

Objectives	Programs
Prepare and Prevent	ID critical infrastructures and interdependencies and address vulnerabilities
Detect and Respond	Detect attacks and unauthorized intrusions
	Develop robust intelligence and law enforcement capabilities consistent with the law
	Share attack warnings and information in a timely manner
	Create capabilities for response, reconstitution, and recovery
Build Strong Foundations	Enhance research and development in the above mentioned areas
	Train and employ adequate numbers of information security specialists
	Make Americans aware of the need for improved cyber-security
	Adopt legislation and appropriations in support of effort
	At every step of the process ensure full protection of American citizens' civil liberties, rights to privacy, and rights to protection of proprietary information

Version 2.0 of the National Plan is to cover the private sector. The Partnership for Critical Infrastructure Protection (see below) is coordinating the private sector's input. The Bush Administration expects to release the next version of the National Plan before the end of the year (2001).

Information Sharing and Analysis Center (ISAC). PDD-63 envisaged an ISAC to be the private sector counterpart to the FBI's National Infrastructure Protection Center (NIPC), collecting and sharing incident and response information among its members and facilitating information exchange between government and the private sector. It is one of the critical recommendations made in the PCCIP and probably one of the hardest to realize. While the Directive conceived of a single center serving the entire private sector, the idea now is that each sector would have its own center. Progress in forming sector ISACs has been mixed.

Twenty-two of the nation's largest banks, securities firms, insurance companies and investment companies have joined together in a limited liability corporation to form a banking and finance industry ISAC. An executive of Bank America chairs the CEO Council that acts as the corporation's board. The group has contracted with an internet service provider[11] (ISP) to design and operate the ISAC. Individual firms feed raw computer network traffic data to the ISAC. The ISP maintains a database and analyzes it for suspicious behavior and provides its customers with summary reports. If suspicious behavior is detected, the analysis may be forwarded to the federal government. Anonymity is maintained between participants and outside the ISAC. The ISP will forward to its customers alerts and other information provided by the federal government. The ISAC became operational in October, 1999.

The telecommunications industry has agreed to establish an ISAC through the National Coordinating Center (NCC). The NCC is a government-industry partnership that coordinates responses to disruptions in the National Communications System. Unlike the banking and finance ISAC that uses a third party for centralized monitoring and analysis, each member firm of the NCC will monitor and analyze its own networks. If a firm suspects its network(s) have been breached, it will discuss the incident(s) within the NCC. The NCC members will decide whether the suspected behavior is serious enough to report to the appropriate federal authorities. Anonymity will be maintained outside the NCC. Any communication between federal authorities and member firms will take place through the NCC, this includes incident response and requests for additional information[12].

The electric power sector, too, has established a decentralized ISAC through its North American Electricity Reliability Council (NAERC). Much like the NCC, NAERC already monitors and coordinates responses to disruptions in the nation's supply of electricity. It is in this forum that information security issues and incidents will be shared. The National Petroleum Council is still considering setting up an ISAC with its members.

In January, 2001, the information technology industry announced its plans to form an ISAC. Members include 19 major hardware, software, and e-commerce firms, including AT&T, IBM, Cisco, Microsoft, Intel, and Oracle. The ISAC will be overseen by a board made up of members and operated by Internet Security Systems.

The country's water authorities are still considering what an appropriate ISAC model might be for their sector. Individual water authorities have existing lines of communications with the FBI through which they could report suspicious behavior. The same could be true for the other local and state emergency services sectors.

In addition to these individual sectors setting up or contemplating ISACs, a number of sectors have formed a **Partnership for Critical Infrastructure Security**

---

[11]The ISP is Global Integrity, a subsidiary of Science Applications International Corp. (SAIC).

[12] Federal agencies sit on the NCC, including the NSA. One could assume that knowledge of incidents discussed in the NCC could find its way to federal investigatory authorities without formally being reported.

to share information and strategies and to identify interdependencies across sectoral lines. The Partnership is a private sector initiative and has filed as a 501(c)(6) organization. A preliminary meeting was held in December 1999 and five working groups were established (Interdependencies/Vulnerability Assessment, Cross-Sector Information Sharing, Legislation and Policy, Research and Development, and Organization). The working groups meet every other month. The federal government is not officially part of the Partnership, but the CIAO acts as a liaison and has provided administrative support for meetings. Sector Liaison from lead agencies are considered ex officio members. Some entities not yet part of their own industry group (e.g. some hospitals and pharmaceutical firms) are interested in participating in the Partnership.

Also, besides the efforts of the lead agencies to assist their sectors in considering ISACs, the NIPC offers private sector firms from across all industries a program called INFRAGARD. The program includes an Alert Network. Participants in the program agree to supply the FBI with two reports when they suspect an intrusion of their systems has occurred. One report is "sanitized" of sensitive information and the other provides more detailed description of the intrusion. The FBI will help the participant respond to the intrusion. In addition, all participants are sent periodic updates on what is known about recent intrusion techniques. The NIPC is working to set up local INFRAGARD chapters that can work with each other and regional FBI field offices. In January, 2001, the FBI announced it had finished establishing INFRAGARD chapters in each of its 56 field offices.

Issues

Administrative. While the Directive deals with infrastructures issues beyond just computer systems and also considers physical protections, the Directive primarily is concerned with "cyber" threats and vulnerabilities and, therefore, is an extension of the government's efforts in computer security. The Directive sought to use existing authorities and expertise as much as possible in assigning responsibilities. Nevertheless, the Directive does set up new entities that, at least at first glance, assume responsibilities previously assigned to others. One question is to what extent does the Directive duplicate, supersede, incorporate, or overturn existing computer security efforts?

For example, the Paperwork Reduction Act of 1995 (P.L. 104-13) placed the responsibility for establishing government-wide information resources management policy with the Director of the Office of Management and Budget. Those policies are outlined in OMB Circular A-130. Appendix III of the Circular incorporates responsibilities for computer security as laid out in the Computer Security Act of 1987.[13] The Computer Security Act requires all agencies to inventory their computer systems and to establish security plans commensurate with the sensitivity of

[13]Appendix III does not apply to information technology that supports certain critical national security missions as defined in 44 USC 3502(9) and 10 USC 2315. Policy for these national security systems, i.e. telecommunications and information systems containing classified information or used by the intelligence or military community, has been assigned by national security directives to the Department of Defense.

information contained on them. Agencies are suppose to submit summaries of their security plans along with their strategic information resources management plan to the Office of Management and Budget (OMB). The agencies are to follow technical, managerial, and administrative guidelines laid out by OMB, the Department of Commerce, the General Services Administration, and the Office of Personnel Management and should include (as detailed in the OMB Circular) incidence response plans, contingencies plans, and awareness and training programs for personnel. The Director of OMB may comment on those plans.

Under PDD-63, agencies submitted plans (not dissimilar in content to those called for in the Computer Security Act of 1987 and detailed in OMB Circular A-130 Appendix III) to the CIAO. The Critical Infrastructure Coordination Group assembled an expert review team to review these plans (an "ad hoc" team was set up at CIAO). What role does the Director of OMB now play in reviewing and commenting on agency plans? What role does the National Coordinator, housed within the National Security Council and to whom the CIAO reports, play in the review and comment of an agency's security plan?[14] Who determines whether an agency's obligation to creating an adequate plan have been met?

Among the responsibilities assigned to the Department of Commerce by OMB Circular A-130 Appendix III is the coordination of agency incident response activities to promote sharing of incident response information and related vulnerabilities. This function has now migrated over to the General Services Administration which has established a Federal Computer Incident and Emergency Response Capability (FedCIRC). But, PDD-63 states and the National Plan reiterates that the National Infrastructure Protection Center will provide the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts. Are the lines of authority clearly established between the different organizations many of which are tasked with doing things that sound similar?[15] What authority or influence will the FBI, as manager of the NIPC, have over these organizations? Also, the NIPC is responsible for warning, responding to, and investigating intrusions. Are these functions compatible?[16]

---

[14]It should be noted that the General Accounting Office has reported that the oversight of agency security measures to date has been inadequate. See, U.S. General Accounting Office, Information Security. Serious Weaknesses Place Critical Federal Operations and Assets at Risk. GAO/AIMD-98-92. Sept. 1998.

[15]In recent testimony to Congress, the General Accounting Office noted that the mission of the NIPC has not been fully defined, leading to differing interpretations by different agencies. Also, the manpower support from and information sharing with other agencies has not materialized as envisioned. See, General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities*. GAO-01-769, Testimony before the Subcommittee on Technology, Terrorism, and Government Information, Senate Judiciary Committee. May 22, 2001.

[16]This point is alluded to by Michael O'Neil, "Securing Our Critical Infrastructure: What Lurks Beyond Y2K," *Legal Times*, Week of Jan. 25, 1999.

The National Plan provides an interesting case in point. The Plan includes a discussion of the Federal Aviation Agency's (FAA) effort in establishing its own Computer Security Incident Response Capability (CSIRC), as a number of other agencies (Department of Energy, National Aeronautics and Space Administration) have done already and which is being promoted by the Directive. The CSIRC is to serve a centralized reporting and monitoring function within FAA. It will carry out FAA-wide intrusion detection, intercepting all network activity that enters each FAA installation. It will support FAA offices by analyzing the intrusion detection data collected. There will be a Computer Incident Response Team (CIRT) trained in handling intrusions and incidents. The CIRT will also provide disaster recovery assistance to restore operations. When the CSIRC detects an intrusion, does it first inform GSA's FedCIRC or the NIPC?[17] Does GSA's FedCIRC function begin helping FAA deal with the intrusion or does the NIPC? Can CSIRC deal with its situation first and then forward information later? Who decides how to balance FAA's need to respond to the intrusion (say kicking the perpetrators off the network) and the FBI's need to gather sufficient evidence to catch and prosecute the perpetrators?

The Computer Security Act of 1987 also established the Computer System Security and Privacy Advisory Board (CSSPAB). The Board reports to the Secretary of Commerce and is tasked with identifying emerging issues relative to computer security and privacy, advising the National Institute of Standards and Technology and the Commerce Secretary on such issues, and reporting to the Secretary of Commerce, the Director of OMB, the Director of the National Security Agency, and appropriate congressional committees. PDD-63 establishes the National Infrastructure Assurance Council. Its duties are to propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes including information and telecommunications systems and monitoring the development of private sector ISACs. The Council will report to the President through the National Coordinator and the Department of Commerce shall act as the President under the Federal Advisory Committee Act. In addition, the National Security Telecommunications Advisory Committee (NSTAC), established by Executive Order 12382 in September 1982, undertook a study back in May 1995 on the reliance of the transportation sector, the electric power sector, and the financial services sector on information networks and the risks to those sectors should those networks be compromised. Are these advisory committees/councils duplicating effort or do they offer complementary viewpoints?

There is another bureaucratic issued raised by PDD-63. Prior to the Computer Security Act of 1987, the Reagan Administration established the National Telecommunications and Information Systems Security Committee.[18] The Committee consists of 22 civilian and defense agencies. The National Security Agency was named National Manager. The Committee was tasked with setting operating policies governing the nation's telecommunications system, its classified information systems, and "other sensitive information." The Computer Security Act of 1987 was enacted

---

[17]The Government Information Security Reform Act, passed as Title X, Subtitle G in the FY2001 Defense Authorization Act (P.L. 106-398) requires agencies to report incidents to GSA.

[18]National Security Decision Directive, NSDD-145. September 17, 1984.

in part out of congressional concern that the Committee might over-classify government-held information[19]. Does PDD-63, by couching critical infrastructures in national security terms and combining DOD and NSA professionals with civilian professionals in operative functions, blur the distinction between classified and unclassified (or national security and civilian) systems which was a primary focus of the Computer Security Act of 1987?[20]

Related to this issue is one raised by some Members of Congress who have questioned the decision to place CIAO within the Department of Commerce. To them, a threat to the nation's critical infrastructures is a national security risk and should be the responsibility of the Department of Defense. The Department of Defense did serve as the executive agent for the PCCIP's Transition Office which was to be the model for National Plan Coordinating Staff function. On the other hand, the Department of Commerce has on-going relationships with many of the private infrastructure operators with whom the Directive hopes to interact.

Restructuring by the Bush Administration. As part of its overall redesign of White House organization and assignment of responsibilities, the new Bush Administration is reviewing its options for coordinating and overseeing critical infrastructure protection. There are three parallel debates that impact this decision.

First, the National Security Council (NSC) is undergoing a major streamlining. All groups within the Council established during previous Administrations have been abolished and must petition for reinstatement. Whether, or to what extent, the NSC will remain the focal point for coordinating critical infrastructure protection (i.e. serve as National Coordinator and chair the Critical Infrastructure Coordination Group) is unclear.

Second, there is continuing debate about the merits of establishing a government-wide Chief Information Officer (CIO), whose responsibilities would include protection of all federal non-national security-related computer systems and coordination with the private sector protection of privately owned computer systems. The Bush Administration recently announced its desire not to create a separate federal CIO position, but to recruit a Deputy Director of the Office of Management and Budget that would assume an oversight role of agency CIOs. One of reason's cited for this was a desire to keep agencies responsible for their own computer security.[21]

Third, there is also continuing debate about how best to defense the country against terrorism, in general. Some include in the terrorist threat cyber attacks on critical infrastructure. The U.S. Commission on National Security/21st Century (the

---

[19]House Report 100-153(I).

[20] This point is made by the Electronic Privacy Information Center in its report, *Critical Infrastructure Protection and the Endangerment of Civil Liberties* (1998) and can be found on the Center's webpage at [http://www.epic.org/security/infowar/epic-cip.html].

[21]For a discussion of this and the status of federal CIO legislation, see CRS Report RL30914, Federal Chief Information Officer (CIO): Opportunities and Challenges, by Jeffery Siefert.

Hart-Rudman Commission) proposed a new National Homeland Security Agency. The recommendation builds upon the current Federal Emergency Management Agency (FEMA) by adding to it the Coast Guard, the Border Patrol, Customs Service, and other agencies. The new organization would include a directorate responsible for critical infrastructure protection. Two bills have been introduced so far in the 107th Congress addressing this issue. H.R. 1292, the Homeland Security Strategy Act of 2001 calls for the President to develop a Homeland Security Strategy that protects the territory, critical infrastructure, and citizens of the United States from the threat or use of chemical, biological, radiological, nuclear, cyber or conventional weapons. H.R. 1158 would establish a National Homeland Security Agency. On May 8, the Bush Administration announced it intention to create a new office within FEMA called the Office of National Preparedness. The Office would act to coordinate all federal programs dealing with weapons of mass destruction consequence management. The announcement also noted the Vice-President Cheney would oversee the development of a plan to address terrorism threats using weapons of mass destruction (WMD). It appears that WMD is limited here to biological, nuclear, or chemical weapons and does not include cyber attacks against critical infrastructures.

Also, it remains to be seen what role the NIPC will play within the Bush Administration given recent criticisms of how that structure is working.[22]

To what extent the Bush Administration commits to other critical infrastructure protection initiatives of the Clinton Administration, such as the scholarship for service program and other federal cyber service programs (see Appendix), FedCIRC, and research and development, also remains to be seen.

Costs. In January, 2000 the Clinton Administration announced it had budgeted $2 billion on critical infrastructure protection for FY2001 (see Appendix). This is an estimate based on inputs to OMB from agencies asked to total and catagorize dollars budgeted for activities related to critical infrastructure protection (e.g. systems protection, training) . It is not clear, though, if agencies are consistent in what they consider relevant. Also, it is difficult to identify some of these expenditures within the agencies' budget submissions and subsequent Congressional appropriations. Much of the $2 billion is buried in other information technology or administrative line items.

Many of the agencies' activities called for immediately by the Directive will be part of on-going administrative duties. These activities, if not previously done (which appears to be the case in many agencies), will require the reallocation of personnel time and effort, presumably at the expense of other activities. The resources required to meet PDD-63 requirements are supposed to be part of the agencies' internal plans. Some of the costs will not be known until after vulnerability assessments are done and remedial actions determined. Also, each agency must develop and implement

---

[22]See, General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities*. GAO-01-769, Testimony before the Subcommittee on Technology, Terrorism, and Government Information, Senate Judiciary Committee. May 22, 2001. See also, *Bush Eyes Overhaul of E-Security*. ComputerWorld. Vol. 34. No. 51. Dec. 18, 2000. pp1,85.

education and awareness training programs. Agency costs may not be insignificant. According to OMB, the IRS alone estimated a vulnerability analysis of its systems will cost $58 million.[23] The Plan outlines efforts at the Department of Energy to improve its network security. Total costs are expected to be $80 million ($45 million for operational security measures). On top of this, the Administration is asking for new initiatives such as the education and training programs (Federal Cyber Service).

Potential private sector costs are also unknown at this time. Some sectors are already at the forefront in computer security and are sufficiently protected or need only marginal investments. Others are not and will have to devote more resources. The ability of certain sectors to raise the necessary capital may be limited, such as metropolitan water authorities which may be limited by regulation, or emergency fire which may function in a small community with a limited resources. Even sectors made up of large well capitalized firms are likely to make additional expenditures only if they can identify a net positive return on investment.

Affecting these business decisions will be issues of risk and liability. As part of its outreach efforts, the CIAO has helped the auditing, accounting, and corporate directors communities identify and present to their memberships the responsibilities governing board of directors and corporate officers have, as part of their fiduciary responsibilities, in managing the risk to their corporation's information assets. The Institute of Internal Auditors, the American Institute of Certified Public Accountants, the Information Systems Audit and Control Association and the National Association of Corporate Directors have formed a consortium and held "summits" around the country in an outreach effort. The main point of their discussion can best be summed up by the following expert from a paper presented at these summits:

> "The consensus opinion from our analysts is that all industries and companies should be equally concerned about information technology security issues because it is an issue that has an enormous potential to negatively impact the valuation of a company's stock...it must be the responsibility of corporate leaders to ensure these threats are actually being addressed on an ongoing basis. At the same time, the investment community must keep the issue front and center of management."[24]

There is also the question of downstream liability, or third party liability. In the denial-of-service attacks that occurred in early 2000, the attacks were launched from "zombie" computers; computers upon which had been placed malicious code that was subsequently activated. What responsibility do the owners of those "zombie" computers have to protect their systems from being used to launch attacks elsewhere? What responsibility do service providers have to protect their customers? According

---

[23]Conversation with OMB officials, 11 February, 1999.

[24]From an paper entitled Information Security Impacting Securities Valuations, by A. Marshall Acuff, Jr., Salomon Smith Barney Inc.

to some, it is only a matter of time before the courts will hear cases on these questions.[25]

Costs to the private sector may also depend on the extent to which the private sector is compelled to go along with PDD-63 versus their ability to set their own security standards. The current thinking is the private sector should voluntarily join the effort and PDD-63 recommends that no new regulations or oversight bodies be formed. But, what happens if a sector does not take actions the federal government feels are necessary?

In an unrelated matter, but one that intersects with the efforts of critical infrastructure protection, the financial services industry and the health care industry are being required to follow new guidelines issued by their regulatory agencies aimed at protecting the privacy of their customer data bases. Pursuant to the Gramm-Leach-Bliley Act of 1999, federal regulators released in February, 2001, guidelines that the industry must follow. Likewise, the Bush Administration is suppose to release by this summer security rules that the health care industry must follow to comply with the 1996 Health Insurance Portability and Accountability Act (HIPPA). The guidelines issued for the financial services industry are general (assess risks, have written policies and procedures to control the risk, implement and test those policies, and update them as necessary). The costs that are associated with these efforts might be a guide for what it would cost if further rules were issued related to protecting information systems upon which the nation's critical infrastructures depend.[26]

Information Sharing. The information sharing called for in PDD-63 — internal to the federal government, between the federal government and the private sector, and between private firms -- raises a number of issues.

PDD-63 calls for information to flow between agencies via FedCIRC and the NIPC. What kind of information will be flowing? Will reporting consist of raw network traffic data or just reports of incidents? Will content be monitored or just the packet headers?[27] Will reporting be in real-time or after-the-fact? How does this impact the privacy and confidentiality of the information provided? The Computer Matching and Privacy Protection Act of 1988 (5 U.S.C. 552a) governs the exchange of records between government agencies. It is not yet clear how the goals of the NIPC and FedCIRC will be impacted by the Act or how the goals of the Act may be impacted if modified to address the NIPC and FedCIRC missions.

---

[25]See, ComputerWorld. *IT Security Destined for the Courtroom.* May 21,2001. Vol 35. No. 21.

[26]For more information on HIPPA, see CRS Report RL30620. *Health Information Standards, Privacy, and Security: HIPPA's Administrative Simplification Regulations*, by Stephen Redhead. For more information on implementation of the Gramm-Leach-Bliley Act, see CRS Report RS20185, Privacy Protection for Customer Financial Information, by Maureen Murphy.

[27]Information travels through the system in packets containing the information itself (content) and a header which contain addresses and instructions on how to handle the information.

Since much of what is considered to be critical infrastructure is owned and operated by the private sector, implementing PDD-63 relies to a large extent on the ability of the private sector and the federal government to share information. However, it is unclear how open the private sector and the government will be in sharing information. The private sector primarily wants from the government information on potential threats which the government may want to protect in order not to compromise sources or investigations. In fact, much of the threat assessment done by the federal government is considered classified.[28] For its part, the government wants specific information on intrusions which companies may hold as proprietary or which they may want to protect to prevent adverse publicity. Success will depend on the ability of each side to demonstrate it can hold in confidence the information exchanged. According to the GAO testimony cited earlier, there is little or no formalized flow of information yet from the private sector to the federal government, in general, or the NIPC specifically.[29]

This issue is made more complex by the question of how the information exchanged will be handled within the context of the Freedom of Information Act (FOIA). Proponents of PDD-63 would hope to exempt the information from public disclosure under the existing FOIA statute. Those more critical of the Directive are concerned that PDD-63 will expand the government's ability to to hold more information as classified or sensitive.[30]

Another question has been raised about the FBI's INFRAGARD program. For example, are firms who volunteer to participate in the program given additional or better information than what is available through the FBI outside the program?

Finally, the information exchanged between private firms within the context of the Sector Coordinators and the ISACS raises antitrust concerns, as well as concerns about sharing information that might unduly benefit competitors.

Privacy/Civil Liberties? The PDD states that individual liberties and rights to privacy are to be preserved as the Directive is implemented. However, on-line monitoring, either for system management reasons or for intrusion detection, has the potential to collect vast amount of information on who is doing what on the network. Once an intrusion is detected, the federal government could get involved in real-time monitoring. What, if any, of that information should be treated as private and subject to privacy laws?

The National Plan states that it was the intent of the Clinton Administration to pass all critical infrastructure efforts through the lens of privacy issues. In addition to promised vigorous and thorough legal reviews of Plan programs, the Plan proposes

---

[28]There are precedents for sharing classified information with private infrastructure operators, and it has been mentioned that these situations might be a model for sharing such information with ISACs and their members, if proper controls are in place. This, however, may involve additional expense and procedural issues for those industries or firms not familiar with handling such information.

[29]Op. Cit. General Accounting Office, Critical Infrastructure Protection.

[30]Op. cit. EPIC

an annual colloquium on Cyber Security, Civil Liberties, and Citizens' Rights between the representatives of the federal government and outside groups.

But members of the privacy and civil liberty communities remain concerned about proposals that have been made. For example, the PCCIP recommended that law enforcement officials should need to get only a single warrant to track hackers through cyberspace, rather than having to get a new warrant every time they trace a hacker to a computer in another jurisdiction. The PCCIP also recommended that employers be allowed to administer polygraph tests to their computer security personnel. There are also suggestions of requiring background checks for computer security personnel. The Clinton Administration did not take a position on any of these recommendations. However, in a hearing before the House Judiciary's Subcommittee on Crime (February 29, 2000), the Clinton Administration did say that having a nationwide track and trace capability would be very helpful in identifying hackers.

Another issue is to what extent will monitoring and responding to cyber attacks permit the government to get involved in the day-to-day operations of private infrastructures? The PCCIP suggested possibly modifying the Defense Production Act (50 USC Appendix, 2061 *et seq*) to provide the federal government with the authority to direct private resources to help reconstitute critical infrastructures suffering from a cyber attack. This authority exists now regarding the supply and distribution of energy and critical materials in an emergency. Suppose that the computer networks managing the nation's railroads were to "go down" for unknown but suspicious reasons. What role would the federal government play in allocating resources and reconstituting service?

Congressional Action

Congress's interest in protecting the nation's critical infrastructure spans its oversight, legislative, and appropriating responsibilities. Most Congressional activity regarding critical infrastructure protection has focused to date on oversight. A number of committees have held hearings on various aspects of the issue. These include the Senate Judiciary's Subcommittee on Technology, Terrorism and Government Information and the Subcommittee on Criminal Justice Oversight, the House Judiciary's Subcommittee on Crime, the Senate Committee on Small Business, the House Science Committee's Technology Subcommittee, the House Government Reform Committee's Subcommittee on Government Management, Information, and Technology, which in September 2000, released a report card rating how well agencies were protecting their information assets.

While there was much activity administratively, on the part of the Clinton Administration, and in oversight by the Congress, legislation has moved more slowly.

In the 106th Congress a number of bills were introduced that addressed one or another issue associated with PDD-63. A couple bills were directly related to PDD-63. S. 2702 required the President to report to Congress on the specific actions being taken by agencies to implement PDD-63. This requirement was later added as an amendment to the FY2001 Department of Defense Authorization Act (P.L. 106-398).

That report which was prepared at the end of the Clinton Administration was released by the Bush Administration in January, 2001. H.R. 4246 directly addressed FOIA and anti-trust concerns associated with ISACs by defining a "cyber security web site" and exempting those websites from FOIA access and anti-trust litigation as long as information contained on those sites are not used to impede free market functions. Also, the bill explicitly allowed the federal government to set up working groups of federal officials to work with industry groups without such groups being considered as federal advisory committees.

Other bills dealt more with computer security in general. S. 1993 amended Chapter 35 USC 44 (related to the Paperwork Reduction Act), to strengthen information security practices throughout the federal government by adding a separate subchapter specifically dedicated to information security. Among other things, the bill requires agencies to have an annual outside assessment of their computer security plans and practices and calls on the Comptroller General to report on those reviews. The bill was attached to the FY2001 Defense Authorization Act (Title X, Subtitle G (referred to as the Government Information Security Reform Act in P.L. 106-398)). Another bill that did not make it into law, H.R. 5024, would have transferred many of the computer security given the Director of OMB by the Paperwork Reduction Act of 1995 to a Government-wide Chief Information Officer located outside OMB.

A number of other bills were introduced that addressed issues such applying trap and trace procedures to tracking hackers across jurisdictions, modifying thresholds and penalties in computer crime statutes, and organizational changes meant to deal better with computer crime and cyber-terrorism. Also, there have been and continue to be a number of other bills introduced that relate to privacy, encryption, public key policies, computer fraud, etc. These issues are tangentially related to PDD-63.[31]

The 107th Congress will undoubtedly continue its oversight of the efforts to protect the nation's critical infrastructure. Also, there may be legislation introduced associated with restructuring the responsibilities for overseeing and coordinating Administration efforts and/or legislation reexamining the criminal statutes and those relating to criminal investigations. Two bills have been introduced associated with homeland defense. H.R. 1292, the Homeland Security Strategy Act of 2001 calls for the President to develop a Homeland Security Strategy that protects the territory, critical infrastructure, and citizens of the United States from the threat or use of chemical, biological, radiological, nuclear, cyber or conventional weapons. H.R. 1158 would establish a National Homeland Security Agency. It is expected that legislation exempting from FOIA information provided the federal government by the private sector concerning computer security and critical infrastructures will also be introduced. Also, hearings have been held on reauthorization of the Defense Production Act (DPA). It remains to be seen if or how the objectives of critical infrastructure protection might be addressed in any DPA reauthorization bills.

---

[31]For an overview of these issues, see CRS Report 98-67, *Internet: An Overview of Six Key Policy Issues Affecting Its Use and Growth*, by Marcia Smith et al.

Appendix

FY2001 Budget

On January 7, 2000, the Clinton Administration announced it was going to ask for $2.03 billion in FY2001for protecting the nation's critical infrastructure against cyber attacks. This was an estimate by OMB, based on canvassing individual agencies to identify activities that constitute protection of their critical infrastructure or support the protection of infrastructure in the private sector. Included in the tally was $621 million for research and development, up from the $461 million that Congress appropriated for FY2000. Among the highlights mentioned in the announcement were a number of initiatives listed below.

Federal Cyber Services Training and Education ($25 million)

This initiative is an effort to improve the recruitment and retention of a highly skilled government information technology workforce, including increasing the pool of skilled information security specialists. The initiative consists of a number of different activities.

One activity would be a ROTC-like program where the federal government, through the National Science Foundation (NSF), will pay for a 2-year undergraduate or graduate degree in information security in exchange for government service in information security, called the Scholarship for Service (SFS). The scholarship would be for two years at schools with accredited information technology programs. Students participating in the program would also do summer internships at government agencies and attend periodic conferences.

A second activity is called the Center for Information Technology Excellence (CITE). CITE would provide continuing training for existing federal systems administrators and information systems security officers. CITE will be managed and run by the Office of Personnel Management. Training will be offered by selected sites both inside and outside the federal government. Curricula will be based on key competencies and a certification process will demonstrate that those competencies have been demonstrated. It should be noted that the National Security Agency runs a similar program geared toward the national security community. NSA has identified 8 universities as centers of information technology excellence. The CITE program identified here would use the experience of the NSA program to establish a similar capability for the entire federal government.

A third activity would be a high school and secondary school outreach program to educate high school students and teachers and the general public about information security. The fourth activity would be to promote information security awareness within the federal workforce.

Permanent Expert Review Team ($5 million over two years)

This would make permanent the review of agencies' internal security plans, vulnerability analyses, etc. The team would be supported through the National Institute of Standards and Technology.

Federal Intrusion Detection Network ($10 million)

FIDNET would be an intrusion detection network for civilian government agencies managed by the General Services Administration. It should be noted that the Department of Defense and the National Security Agency have each set up their own intrusion detection networks. These will all be linked together and with the National Infrastructure Protection Center at the FBI.

Public Key Infrastructure Pilots ($7 million)

Public key infrastructure (PKI) allows two-way authentication of communications over computers and is critical for electronic commerce and for agency to exchange information with contractors, constituents, etc. This initiative would support 7 pilot programs at different federal agencies.

Institute for Information Infrastructure Protection ($50 million)

This would be a research and development fund operated through the National Institute of Standards and Technology (NIST) to support research that might not otherwise be conducted by the private sector or defense agencies. Currently nearly all of the current information security research and development funds go to defense agencies. While operated through NIST, the Institute would report to a Federal Coordinating Council consisting of the President's Science Advisor, the Deputy Director/ Office of Management and Budget, the Director/National Security Agency, the Director/NIST, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. The Institute would consult with the National Infrastructure Advisory Council and the Sector Coordinators.

Since much of the estimated $2.0 billion budgeted for critical infrastructure protection falls within ongoing administrative accounts, it is difficult to track the extent to which these activities are supported by appropriations until (or unless) OMB releases a FY2002 budget identifying how expenditures were allocated in FY2001. However, a couple of initiatives were more highly visible and Congress provided mixed support for them. For example, the NSF scholarship for service program received its $11.2 million appropriation. NIST did not receive the $50 million appropriation for the Institute for Information Infrastructure Protection, but did receive $3 million of the $5 million requested for the Expert Review Team. GSA received $8 million of the $15 million it requested for FIDNET and FedCIRC. How much of that goes toward FIDNET is not clear.

Table A.1. Critical Infrastructure Protection Funding by Department

(millions $)

Department	FY98 actual	FY99 actual	FY00 enacted	FY01 request
Agriculture	2.70	3.22	3.88	14.03
Commerce	9.35	21.81	17.75	92.10
Education	3.59	4.45	5.23	2.51
Energy	1.50	3.60	21.98	45.30
EOP	0.05	0.58	0.48	0.56
EPA	0.12	0.24	0.08	2.3
FEMA	0.00	0.00	0.80	1.47
GSA	0.00	3.00	0.00	15.40
HHS	21.83	12.17	13.17	19.55
Interior	1.29	1.60	2.65	1.83
Justice	25.61	54.09	44.02	45.51
NASA	41.00	43.00	66.00	61.00
NSF	19.15	21.42	26.65	43.85
National Security (incl. DOD)	974.56	1,185.22	1,402.94	1458.91
Nuclear Regulatory Commission	0.00	0.20	0.00	0.25
OPM	0.00	0.00	2.00	9.00
Transportation	20.33	24.88	50.68	92.34
Treasury	22.91	48.89	76.22	87.03
Veteran’s Affairs	0.00	0.00	17.33	17.39
Grand Total	**1,143.98**	**1,428.35**	**1,751.86**	**2,010.33**

\ data from Office of Management and Budget